SUBJECT: Network Monitoring – Revalidated May 8, 2014

RESPONSIBLE OFFICE: MI/Chief Information Officer

1. POLICY

a. It is Center policy that electronic communications shall be monitored continuously to ensure the proper use of Information Technology (IT) resources by its workforce, to gauge the performance and availability of its networks and services, and to secure its data and information systems from hostile intrusions, misuse, and other threats. The function of monitoring Center networks and services will be limited to the Office of the Chief Information Officer (OCIO) Network and Information Technology (IT) Security personnel, and will be conducted as follows:

(1) The OCIO network personnel shall be responsible for routine monitoring of all Dryden networks and services to ensure availability and performance including remote sites.

(2) The OCIO IT security personnel shall be responsible for detecting intrusions, monitoring for illegal software and malicious code, and monitoring for unauthorized network devices, services, ports, or protocols. If suspicious traffic, criminal or noncriminal, is discovered during routine monitoring, incident response policies will be followed.

b. The monitoring (encrypted or unencrypted) of inbound or outbound traffic on the Center network shall be based on risk management principles, with a higher concentration on those assets deemed most critical to NASA.

c. Center IT resources are the property of the U.S. Government; therefore, the Center shall monitor all aspects of computer usage at any time. Monitoring includes the following activities.

(1) Monitoring can include ports, IP addresses, protocols, and content. Monitoring shall be performed either by automated means, such as intrusion detection systems and flow-based content monitors, or by manual inspection of the contents of captured

network data or log data. A diverse and dynamic range of computer tools are used and tested to perform monitoring activities.

(2) All Network Monitoring and Intrusion Detection Logs shall be centrally managed. Access to the monitoring systems and central log system will be restricted to authorized OCIO network and IT security personnel. All logs and information collected by network monitoring tools will be maintained and preserved in accordance with NPR 1441.1, NASA Records Retention Schedule, and will be properly safeguarded and not released beyond the OCIO network and IT security personnel unless approved by the Center CIO.

(3) All requests for network monitoring shall be coordinated with Center Information Security Officer (CISO).

2. APPLICABILITY

a. This policy applies to Armstrong Flight Research Center (AFRC) civil servants and on-site support contractors, grant recipients, and other partners to the extent specified in their contracts or agreements.

3. AUTHORITY

a. NPR 2810.1, Security of Information Technology

4. REFERENCES

a. NPD 1441.1, NASA Records Retention Schedule

b. NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology

5. RESPONSIBILITY

a. The Center CIO is responsible for maintaining responsibility and accountability for Center-specific implementation of the network monitoring program; informing the Center Director, as appropriate, of monitoring activity and findings; and reviewing and approving testing agreements and protocols for evaluations of monitoring technology in the Center network environment.

b. The CISO is responsible for reviewing suspicious activities identified during routine monitoring to determine the course of action; notifying law enforcement of suspected criminal activities identified during monitoring; reviewing and approving requests for targeted monitoring from authorized NASA managers and law enforcement officials; maintaining documentation of all targeted monitoring activities involving the Center, including law enforcement or other requests for targeted monitoring and receipts for

targeted monitoring records; and informing Center managers and the Center CIO, as appropriate, of the results of targeted monitoring.

c. The OCIO Network and IT Security Personnel are responsible for conducting monitoring as directed under the NASA IT security monitoring program; maintaining audit logs of all routine monitoring activities, as well as identified suspicious activities recommended for further targeted monitoring; reporting to the CISO or other appropriate management chain any suspicious activity identified during routine monitoring; providing technical support and monitoring services for approved targeted monitoring activities; informing the CISO on the progress and results of targeted monitoring; providing records of approved targeted monitoring to the requestor; and properly safeguarding all data collected from monitoring.

6. DELEGATION OF AUTHORITY
None

7. MEASUREMENTS
None

8. CANCELLATION
None

Revalidated May 1, 2014. Original signed by

/S/ David McBride

ATTACHMENT A: Acronyms

AFRC	Armstrong Flight Research Center
CISO	Chief Information Security Officer
IP	Internet Protocol
IT	Information Technology
NASA	National Aeronautics and Space Administration
OCIO	Office of the Chief Information Officer

DISTRIBUTION
Approved for release via the DFRC Document Library; public distribution is unlimited.

Document History Log
Review Date:

This page is for informational purposes and does not have to be retained with the document.

Status Change	Document Revision	Effective Date	Description of Change
Baseline		05/01/09	
Admin Change	Baseline-1	07/23/09	• Added serial number to document name. Name changed from DPD-2810.1 to DPD-2810.1-001. The content did not change.
Admin Change	Baseline-2	12/10/09	• Replaced reference to cancelled document DPD-2800.1-001, Personal Use of Government Office Equipment Including Information Technology, with reference to NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology
Admin Change	Baseline-3	07/13/10	• Changed Code V to Code MI • Changed formatting to comply with Agency standards
Revalidated	Baseline-3	05/01/14	• Changed all references to Dryden and DFRC to Armstrong and Center • Changed ITSM to CISO • Added Attachment A: Acronyms